Cultures & Conflits

76 | hiver 2009
Fichage et listing

La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ?

The fight against "dirty money" from the perspective of fundamental freedoms: which mobilisations?

Anthony Amicelle et Gilles Favarel-Garrigues

Édition électronique
URL : http://journals.openedition.org/conflits/17768
DOI : 10.4000/conflits.17768
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 15 décembre 2009
Pagination : 39-66
ISBN : 978-2-296-11655-9
ISSN : 1157-996X

Référence électronique
Anthony Amicelle et Gilles Favarel-Garrigues, « La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ? », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011, consulté le 30 avril 2019. URL : http://journals.openedition.org/conflits/17768 ; DOI : 10.4000/conflits.17768

La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ?

Anthony AMICELLE, Gilles FAVAREL-GARRIGUES

Anthony Amicelle est doctorant en science politique à l'IEP de Paris, rattaché au Centre d'études et de recherches internationales (CERI), chercheur associé au Centre d'études en sciences sociales de la défense (C2SD/IRSEM). Il est actuellement chargé d'enseignement en relations internationales à l'IEP de Lille. Ses recherches portent sur les politiques européennes et internationales en matière de lutte contre le financement du terrorisme et le blanchiment d'argent, sur les enjeux et usages de la surveillance financière et plus généralement sur les études de sécurité.

Gilles Favarel-Garrigues est chercheur CNRS au Centre d'études et de recherches internationales de Sciences Po. Ses travaux portent sur le changement de politique pénale en Russie et sur les mobilisations internationales contre les grandes menaces criminelles. Il a récemment publié, avec Thierry Godefroy et Pierre Lascoumes, Les sentinelles de l'argent sale. Les banques aux prises avec l'anti-blanchiment, *Paris, La découverte, 2009.*

Toutes les stratégies actuelles de lutte contre le terrorisme et les délinquances transnationales comportent un volet financier qui promeut une surveillance accrue des mouvements de capitaux. Les mesures mises en œuvre prennent diverses formes, parmi lesquelles se distinguent l'imposition de sanctions économiques ciblées (« listes noires »), la communication transnationale de données personnelles et la délégation à des acteurs privés de prérogatives policières. Plus de 170 juridictions nationales sont aujourd'hui engagées dans la lutte contre le blanchiment et le financement du terrorisme. Dans chacune de ces juridictions, l'action gouvernementale s'appuie sur la vigilance des institutions privées chargées de détecter les transactions et les clients suspects et de transmettre les informations pertinentes aux services de renseignements compétents. Il s'agit en premier lieu des banques, mais bien d'autres professions sont aujourd'hui concernées (compagnies d'assurances, offices de notaires, cabinets d'avocats, etc.). Les établissements bancaires ont ainsi dû

concevoir et mettre en œuvre des procédures de surveillance de la clientèle au nom des missions que les gouvernements leur demandent d'assumer.

Evoluant au gré de l'agenda politique du GAFI (Groupe d'action financière) [1], la lutte contre l'argent sale a vu son champ d'action s'élargir, allant du trafic de drogues à la prolifération nucléaire en passant par la priorité continue donnée à l'antiterrorisme. Cette plasticité des cibles a aiguillé dans le même temps la formation des modalités d'intervention. A l'image de la lutte antiterroriste dans son ensemble, les pratiques de surveillance financière ont officiellement endossé des fonctions aussi bien investigatrices qu'analytiques et proactives. De ce point de vue, plus qu'un simple indice permettant la confiscation de capitaux illicites, l'information financière constitue désormais un outil de renseignement clé dans la lutte contre la violence erratique [2]. Contrastant avec les cibles mouvantes de la lutte contre l'argent sale, la finalité revendiquée de ce dispositif renvoie inéluctablement au même objet qu'il convient de sécuriser, à savoir l'intégrité du système financier [3]. La surveillance des flux de capitaux s'apparente à une « gouvernementalité de la mobilité [4] » qui érige les institutions bancaires en filtres protecteurs de l'architecture financière internationale. Ces filtres procèdent à l'évaluation différentielle des risques devant mener à l'exclusion des flux « illégitimes » sans obstruer la fluidité systémique des mouvements d'argent.

De cette gestion sécuritaire des flux financiers, basée sur l'identification de catégories à risque et la mise au ban des opérateurs illégitimes, découle une série de mises en tension au regard des libertés fondamentales qui mérite d'être étudiée. Dans une perspective de « sociologie de la critique [5] », nous proposons d'examiner la publicité accordée à certaines transgressions de normes, avérées ou supposées, et à l'inverse le peu de réactions suscitées par d'autres. Les pratiques de lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi que leur impact sur les droits fondamentaux, se distinguent en

1 . Organisme intergouvernemental visant à développer et promouvoir des politiques nationales et internationales afin de lutter contre le blanchiment de capitaux et le financement du terrorisme. Cf. www.fatf-gafi.org

2 . Sur la stratégie du Royaume-Uni, cf. notamment H.M Treasury, *The financial challenge to crime and terrorism*, 28 février 2007, www.hm-treasury.gov.uk/fin_money_financialchallenge.htm. Sur la stratégie européenne inspirée par la politique britannique, cf. Conseil de l'Union européenne, *Stratégie révisée de lutte contre le financement du terrorisme*, Bruxelles, 17 juillet 2008.

3 . Cf. Mitsilegas V., "Countering the chameleon threat of dirty money" in Edwards A., Gill P. (eds.), *Transnational Organized Crime: Perspectives on global security*, New York, Routledge, 2003, p. 199. Au niveau européen, l'intitulé officiel de la « troisième directive anti-blanchiment » illustre bien cette focale : Directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

4 . Bigo D., Bocco R., Piermay J-L., « Introduction. Logiques de marquage : murs et disputes frontalières », *Cultures & Conflits*, n° 73, 2009, pp. 7-13.

5 . Cf. Boltanski L., Claverie E., « Du monde social en tant que procès » in Boltanski L., Claverie E., Offenstadt N., Van Damme S. (dir.), *Affaires, scandales et grandes causes : De Socrate à Pinochet*, Paris, Stock, 2007, p. 411.

effet par une visibilité variable. Les cas les plus « scandaleux [6] » font incontestablement référence aux listes nominales officielles qui correspondent d'ailleurs à une stratégie de « *naming and shaming* », c'est-à-dire basée sur une réprobation publique. Le cas de l'« affaire SWIFT », qui illustre les dangers liés à la diffusion d'informations personnelles confidentielles, est déjà plus ambigu car la mobilisation critique est restée limitée. Enfin le contraste entre l'attention accordée aux « listes noires » et l'invisibilité relative qui caractérise les usages des technologies de surveillance fondées sur le profilage dans les banques est particulièrement saisissant. Partant donc du postulat que scandales et affaires s'originent dans des dénonciations publiques [7], l'article met en perspective l'ampleur variable des réactions suscitées par les actes de désapprobation visibles dans les trois cas de figure de la lutte contre l'argent sale. Pour ce faire, cette enquête associe les résultats empiriques des recherches menées distinctement par les deux auteurs ; l'une sur l'institutionnalisation progressive du rôle des banques dans l'anti-blanchiment en France et en Suisse [8], l'autre sur les mesures européennes contre le financement du terrorisme [9]. Des entretiens conduits auprès de la CNIL (Commission nationale de l'informatique et des libertés) et auprès d'individus inscrits sur les « listes terroristes » européennes ainsi que leurs avocats viennent compléter la mise en commun de ces travaux. Notre démarche consiste à décrire les trois « épreuves » en donnant à voir et en mettant en relation les appuis normatifs développés par les parties en présence. Dès lors, les trois pratiques de surveillance financière étudiées offrent à l'analyse trois positionnements différents sur le continuum allant du scandale à l'affaire. En retranscrivant l'incertitude qui a entouré le déroulement de ces événements, notre ambition est de donner des clés de compréhension à l'égard des dynamiques de mobilisation. Il s'agit en dernière instance de rendre intelligible l'issue indéterminée de ces « propositions d'engagement » en confrontant les rapports qu'entretiennent les divers acteurs avec les transgressions de normes dénoncées et leurs problématisations.

La mise à l'épreuve des « listes noires »

Dans le sillage des événements du 11 septembre 2001, le décentrage de la lutte contre l'argent sale vers le financement du terrorisme a remis au goût du jour le recours aux « listes noires ». Certains Etats et instances supranationales ont ainsi publié leurs propres listes nominales, et l'usage de celles qui exis-

6 . L'emploi de la notion de « scandale » renvoie à sa conceptualisation en tant qu'épreuve débutant par un acte de dénonciation publique et dont l'importance ou la relativisation dépend de la réaction collective qu'elle suscite. Cf. notamment De Blic D., Lemieux C., « Le scandale comme épreuve : éléments de sociologie pragmatique », *Politix*, vol. 3, n° 71, 2005, pp. 9-38.

7 . *Ibid.*

8 . Favarel-Garrigues G., Godefroy T., Lascoumes P., *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris, La Découverte, 2009.

9 . Amicelle A., *L'Union européenne dans la lutte contre le financement du terrorisme. Enjeux et usages d'un dispositif de gestion des flux financiers*, thèse en cours de rédaction.

taient d'ores et déjà avant 2001 a été considérablement renforcé.

Désigner et geler

S'appuyant sur l'action publique initiée sous l'administration Clinton [10], la promulgation du décret présidentiel 13224, le 23 septembre 2001, a représenté la mesure la plus visible, donnant corps à la rhétorique américaine de « guerre contre le terrorisme ». 27 individus et organisations – présumés liés, directement ou indirectement, aux activités d'Al-Qaida et de groupes associés – ont été listés sous la qualification de *specially designated global terrorists* et leurs avoirs ont été bloqués. D'abord complétée toutes les quatre semaines, cette liste sera, dès la fin de l'année 2001, composée de 158 entités. Dans le même temps, ces désignations nationales vont être « multilatéralisées » sous l'égide de l'ONU en étant pour la plupart ajoutées à la liste onusienne déjà existante, donnant ainsi une « validité universelle » aux sanctions américaines [11]. Liste déjà existante car le 15 octobre 1999, le Conseil de sécurité des Nations unies avait adopté la résolution 1267 concernant Al-Qaida, les Taliban puis les personnes et entités qui leur sont associées, et mettant en place le « comité 1267 ». Ce dernier, composé des 15 membres du Conseil de sécurité, est chargé de superviser l'application de la résolution en désignant les personnes et organisations soumises à ce nouveau régime de sanctions financières. Placé au cœur des activités antiterroristes à la suite du 11 septembre 2001, ce régime de sanctions a été modifié par une myriade de résolutions ultérieures. Parmi celles-ci, la résolution 1390, adoptée en janvier 2002, marque un tournant car elle implique que l'entité ciblée ne doit plus nécessairement être reliée à un territoire étatique particulier (l'Afghanistan précédemment). Autrement dit, si elle n'est pas la première résolution visant des acteurs non-étatiques [12], elle s'affirme en revanche comme la seule renvoyant à une forme de sanction déterritorialisée. Le règlement n° 881/2002 du Conseil de l'Union européenne est d'ailleurs venu la mettre en œuvre dans le cadre européen, transposant du même coup la liste consolidée des Nations unies [13]. Antérieurement à la reprise *in extenso* de cette liste, l'Union européenne (UE) s'est également pourvue en décembre 2001 de sa propre liste indépendante, en se prévalant de la résolution 1373 du Conseil de sécurité adoptée le 28 septembre 2001 sur la

10 . Sur les débuts, dans les années 1990, des sanctions ciblant des « terroristes » ainsi que leur financement, et ouvrant la porte à un usage étendu de sanctions économiques contre des acteurs non-étatiques, cf. Eckert S. E., "The US regulatory approach to terrorist financing" in Biersteker T. J., Eckert, Sue E. (eds.), *Countering the Financing of Terrorism*, New York, Routledge, 2007, pp. 209-233.

11 . Cameron I., "Protecting Legal Rights: On the (in)security of targeted sanctions" in Wallensteen P., Staibano C. (eds.), *International Sanctions: between Words and Wars in the Global System*, New York, Frank Cass, 2005, p. 194.

12 . Voir notamment sur les résolutions au sujet de l'UNITA en Angola : Cameron I., *op.cit.* ; Cortright D., Lopez G. A., *Smart Sanctions: Targeted Economic Statecraft*, Lanham, Md., Rowman and Littlefield, 2002.

13 . Règlement (CE) n°881/2002 du Conseil du 27 mai 2002 instituant certaines mesures spécifiques à l'encontre de certaines personnes et entités liées à Oussama ben Laden, au réseau Al-Qaida et aux Talibans, *J.O. des Communautés européennes* (*JOCE*), L 139/9, 29 mai 2002.

suppression du financement du terrorisme [14].

Au-delà des attentes dissuasives et répressives envers les « listes noires », la place accordée à l'approche « désigner et geler » s'explique en grande partie par sa dimension symbolique. Au lendemain du 11 septembre, les professionnels de la politique et de la sécurité ont considéré ces listes comme un instrument permettant de rendre rapidement visible des actions concrètes fortes aux résultats quantifiables. Censées démontrer les capacités de réactions gouvernementales, ces désignations publiques ont même, pendant un temps, été érigées au rang d'étalon de mesure de l'efficacité antiterroriste via l'accent porté sur les montants gelés [15]. Le message de détermination que les Etats-Unis, mais aussi les autres membres du Conseil de sécurité et l'UE, souhaitaient véhiculer par le biais des listes a néanmoins dû rapidement faire face à la montée en puissance d'une « opinion critique » autour des mécanismes de désignation et de radiation. Des officiels du Trésor américain ont d'ailleurs reconnu l'emballement post-11 septembre qui a pesé sur les premières désignations, évoquant la faiblesse de certaines « preuves » confidentielles ayant justifié ces décisions [16]. Des études ont révélé l'étendue des conséquences de certaines inscriptions prématurées, que ce soit via la stigmatisation de systèmes informels de transfert de fonds [17] ou du travail d'ONG, notamment d'organisations de bienfaisance musulmanes [18]. Plus généralement, cette mise à l'épreuve des « listes noires » s'est principalement adossée à un registre juridique relayé par les nombreuses actions dont a été saisie la Cour européenne de Justice.

14 . La résolution 1373 est d'une importance capitale puisqu'elle requiert la criminalisation de tout soutien apporté à des « terroristes », le gel des fonds suspects ou encore le partage d'informations opérationnelles. Cependant, cette résolution ne prévoit pas, en tant que telle, la création de listes. Position commune 2001/931/PESC du Conseil du 27 décembre 2001 relative à l'application de mesures spécifiques en vue de lutter contre le terrorisme, *JOCE*, L 344/93, 28 décembre 2001 ; Règlement n°2580/2001 du Conseil du 27 décembre 2001 concernant l'adoption de mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le terrorisme, *JOCE*, L 344/70, 28 décembre 2001.

15 . Cf. par exemple Biersteker T. J., Eckert S. E., Romaniuk P., "International initiatives to combat the financing of terrorism" in Biersteker, Thomas J.et Eckert, Sue E. (eds), *Countering the Financing of Terrorism*, New York, Routledge, 2007, p. 245.

16 . Roth J., Greenburg D., Wille S., *National Commission on Terrorist Attacks upon the United State. Monograph on Terrorist Financing* (Staff Report to the Commission), 2004, www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf

17 . Sur le cas *Al-Barakaat* (du nom de la compagnie qui représentait le plus important système de remise de fonds opérant en Somalie avant d'être « blacklistée » par le Trésor américain en novembre 2001), cf. Maimbo S., Passas M., "The design, development, and implementation of regulatory and supervisory frameworks for informal funds transfer systems" in Biersteker T. J., Eckert S. E. (eds.), *Countering the Financing of Terrorism*, New York, Routledge, 2007, pp. 179-182 ; Warde I., *Propagande impériale et guerre financière contre le terrorisme*, Marseille, Agone, 2007, pp. 189-199.

18 . ACLU (*American Civil Liberties Union*), *Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the War on Terrorism Financing*, rapport du 16 juin 2009. http://www.aclu.org/intlhumanrights/nationalsecurity/39849pub20090616.html

Un monde kafkaïen : l'émergence d'une cause

Les acteurs qui endossent un rôle de médiation et font appel à l'« opinion » ont très souvent eu recours à la figure de Kafka et à son ouvrage *Le procès*, afin d'illustrer par la métaphore leurs arguments de dénonciation des procédures sous-tendant l'établissement des « listes de terroristes » [19]. S'ils mettent en récit des cas individuels, ces « *opérateurs de mise à l'épreuve d'un sens commun de l'injustice* [20] » le font au profit d'une montée en généralité arguant que leur histoire « *n'est qu'une parmi d'autres* [21] ». En effet, ils ont insisté sur l'opacité originelle des processus d'inclusion et d'exclusion qui tranche avec la survisibilité des « listes noires ». A partir de sa création en décembre 2001, la gestion de la liste européenne autonome a par exemple dépendu des recommandations provenant de ce que certains officiels de la Commission ont appelé, non sans ironie, la « *non-existent clearing house* [22] ». Les réunions de ce groupe informel ont fait office de mécanisme de consultation des demandes d'Etats membres et de pays tiers proposant des noms à enregistrer, la liste de noms étant ensuite formellement approuvée par le Coreper [23], puis adoptée et publiée sans trop de discussions par le Conseil de l'UE. A l'issue de ce cheminement, les personnes et organisations retenues étaient donc portées sur la liste mais sans que ne leur soient communiquées, au moins jusqu'en 2007, ni leur inscription ni les raisons justifiant cette décision synonyme de mesures restrictives. Des associations de défense des droits de l'Homme, telles qu'*Amnesty International* (dans son rapport de 2005), ont dénoncé le manque de transparence des procédures de *listing/delisting* et ses conséquences sur les droits fondamentaux au travers de cas emblématiques [24]. Si la base légale de la

19 . A titre d'exemple : « *L'histoire qui suit semble sortir d'un livre de Kafka. Hélas, il s'agit bien de faits réels qui se passent au XXIe siècle dans des pays membres du Conseil de l'Europe, sous l'égide de l'organisation des Nations unies* », Assemblée parlementaire du Conseil de l'Europe (Commission des questions juridiques et des droits de l'Homme), « Listes noires du Conseil de sécurité des Nations Unies », note publiée en mars 2007, (propos introductifs).

20 . Pour reprendre l'expression employée par Boltanski L., Claverie E., « Du monde social en tant que procès », *op.cit.*, p. 413.

21 . Assemblée parlementaire du Conseil de l'Europe, *op.cit.*, p. 1.

22 . Entretien avec un officiel de la Commission européenne et un expert national détaché, Bruxelles, mars 2006. Bien qu'il n'y ait pas de règles fixes, cette *clearing house* fut composée pour l'essentiel de délégués des ministères des affaires étrangères et des services de renseignement des Etats membres.

23 . Le Coreper (ou Comité des représentants permanents) est chargé de préparer les travaux du Conseil de l'UE. Composé des ambassadeurs des Etats membres auprès de l'UE, il est présidé par l'Etat membre qui assure la présidence du Conseil.

24 . Amnesty International évoque notamment le cas de Jose Maria Sison (Amnesty International EU Office, *Human rights dissolving at the borders? Counter-terrorism and EU criminal law*, rapport du 30 mai 2005, pp. 6-8, www.amnesty.org/en/library/asset/IOR61/013/2005/en/ab320693-d4e3-11dd-8a23-d58a49c0d652/ior610132005en.html. Citation (traduite, p. 8) résumant l'argumentation du rapport sur ce sujet : « *L'incapacité d'avoir accès aux documents relatifs à la décision d'inclure une personne sur la liste a pour effet de saper la possibilité pratique de former un recours contre cette inclusion. Il est impossible de contester une inclusion si ses raisons demeurent inconnues* ». La commission des questions juridiques et des droits de l'Homme de l'Assemblée parlementaire du Conseil de l'Europe se focalise principalement sur le cas de Youssef Nada (Assemblée parlementaire du Conseil de l'Europe, *op.cit.*).

liste exclut toute réelle évaluation par le Parlement européen et ses pairs nationaux, certains recours formés devant le tribunal de première instance des Communautés européennes ont au contraire abouti aux premières annulations de décisions du Conseil [25]. Si ces arrêts importants n'ont pas impliqué un retrait de la liste pour les requérants, ils ont en revanche poussé le Conseil à procéder à un premier réexamen des mécanismes d'inscription et de radiation [26]. Dans le verdict prononcé en décembre 2006 ayant annulé la décision du Conseil ordonnant le gel des fonds de l'Organisation des Modjahedines du peuple iranien (arrêt OMPI), le tribunal de première instance a ainsi considéré que « *la décision attaquée viole les droits de la défense, l'obligation de motivation et le droit à une protection juridictionnelle effective* ». Par la suite, les procédures ont donc été quelque peu modifiées, avec notamment : la formalisation de l'existence et des fonctions de la *clearing house* sous l'intitulé « Groupe PC 931 [27] » (ses travaux et sa composition restant confidentiels) ; la nécessaire rédaction d'un exposé des motifs devant justifier l'inscription sur la liste ; l'obligation d'envoyer une lettre de notification aux intéressés les informant des mesures prises à leur encontre, de l'exposé des motifs et de leur droit de recours. Outre cet impact jurisprudentiel pionnier, la trajectoire du cas OMPI s'avère être particulièrement révélatrice des tensions à l'œuvre entre décisions de justice et décisions du Conseil qui continuent de persister après ce réexamen procédural [28].

Concomitante des rapports de force à propos de la liste autonome, cette tension autour des mécanismes de désignation et de radiation s'est cristallisée sur l'autre liste européenne : celle par laquelle a été transposé le régime de sanctions onusien. De ce point de vue, le cas de Yassin Abdullah Kadi constitue indéniablement un des éléments catalyseurs sur lequel a pris appui la critique. Cet homme d'affaires saoudien a été désigné, le 19 octobre 2001, par le « comité 1267 » comme étant associé à Oussama ben Laden, Al-Qaida ou les Talibans et ses comptes bancaires ont été gelés. Comme une douzaine d'autres inscrits, M. Kadi a contesté son inclusion dans cette liste devant les tribunaux européens. Après un premier arrêt ambivalent du tribunal de première instance, la Cour européenne de Justice a annulé en appel le règlement du Conseil gelant les fonds de l'intéressé [29]. Reconnaissant une violation des droits de la défense, la Cour entend surtout signifier « *que les juridictions communautaires*

25 . Arrêt du Tribunal de première instance dans l'affaire T-228/02 *Organisation des Modjahedines du peuple d'Iran/Conseil de l'UE*, 12 décembre 2006 ; arrêts du tribunal de première instance dans les affaires T-47/03 et T-327/03 *Jose Maria Sison/Conseil de l'UE*, *Stiching Al-Aqsa/Conseil de l'UE*, 11 juillet 2007.

26 . Cf. Conseil de l'UE, *Fight against the financing of terrorism - Implementation of Common Position 2001/931/CFSP*, Bruxelles, 10826/1/07, 28 juin 2007.

27 . Du nom de la Position Commune 2001/931/PESC à l'origine de la liste.

28 . Voir à cet égard l'arrêt très instructif du 4 décembre 2008 qui annule, pour la troisième fois, une décision du Conseil gelant les fonds de l'OMPI et aboutit finalement, en janvier 2009, au retrait du groupe de la liste communautaire. Arrêt du Tribunal de première instance dans l'affaire T-284/08, *People's Mojahedin Organization of Iran/Council*, communiqué de presse n°84/08, 4 décembre 2008.

sont compétentes pour contrôler les mesures adoptées par la Communauté qui mettent en œuvre des résolutions du Conseil de sécurité des Nations unies [30] ». Bien qu'il ne se prononce nullement sur la décision du Conseil de sécurité au fondement des mesures imposées à M. Kadi et qu'il n'induise pas la radiation de ce dernier, cet arrêt du 3 septembre 2008 alimente la controverse au sujet de la liste ONU [31]. Outre les débats sur un éventuel conflit entre ordres juridiques européen et international [32], ce cas a focalisé l'attention sur le fait que les personnes et entités listées peuvent l'être pour des motifs fondés sur des renseignements classés confidentiels et donc partiellement inaccessibles aux personnes suspectées. Au fil des ans, de nombreux rapports ont insisté sur ce qui est assimilé à un écart indigne entre d'un côté les exigences requises par les standards de *listing* et de l'autre la garantie des droits fondamentaux des individus [33]. Qu'elles soient modérées ou extrêmement virulentes, ces mises en accusation prennent la forme de « critiques internes » qui, même si elles ne remettent pas en cause l'idée des sanctions ciblées, jugent l'Organisation des Nations unies au regard de ses propres principes [34]. Des réformes ont pourtant été engagées au gré des résolutions [35], mais, perçues comme insuffisantes, elles n'ont pas apaisé les tensions qui ont poussé une coalition d'Etats européens à préconiser, auprès du Conseil de sécurité, un système de révision judiciaire indépendante des décisions de *listing/delisting* [36]. Les discussions conti-

29 . Arrêt du Tribunal de première instance dans les affaires T-306/01 et T-315/01, *Ahmed Ali Yusuf et Al Barakaat International Foundation et Yassin Abdullah Kadi/Conseil de l'UE et Commission des Communautés européennes*, communiqué de presse n°79/05, 21 septembre 2005 ; arrêt de la Cour dans les affaires jointes C-402/05 P et C-415/05 P, *Yassin Abdullah Kadi et Al Barakaat International Foundation/Conseil et Commission*, communiqué de presse n°60/08, 3 septembre 2008.

30 . *Ibid.*

31 . Suite à un recours analogue, le tribunal de première instance a également annulé, le 11 juin 2009, la décision du Conseil gelant les fonds d'Omar Mohammed Othman. Arrêt du Tribunal de première instance dans l'affaire T-318/01, *Omar Mohammed Othman/Conseil et Commission*, communiqué de presse n°53/09, 11 juin 2009.

32 . Voir par exemple : Chatham House, *UN and EU Sanctions: Human Rights and the Fight against Terrorism - The Kadi case, Summary of the Chatham House International Law Discussion Group*, 22 janvier 2009, www.chathamhouse.org.uk/files/13293_il220109.pdf

33 . A titre d'exemples : Watson Institute for International Studies, Targeted Sanctions Project, *Strengthening Targeted Sanctions*, 2006, www.watsoninstitute.org/project_detail.cfm?id=4 ; Marty D. (Rapporteur), *Report : United Nations Security Council and European Union blacklists*, Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe, 16 novembre 2007 ; International Commission of Jurists, *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights*, 2009, news.bbc.co.uk/2/shared/bsp/hi/pdfs/16_02_09_ejp_report.pdf

34 . Sur la notion de critique interne et sa distinction de critique externe, cf. Lemieux C., *Mauvaise presse, une sociologie compréhensive du travail journalistique et de ses critiques*, Paris, Métailié, 2000 ; Linhardt D., « Epreuve terroriste et forme affaire : Allemagne, 1964-1982 » in Boltanski L., Claverie E., Offenstadt N., Van Damme S. (dir.), *Affaires, scandales et grandes causes : De Socrate à Pinochet*, Paris, Stock, 2007, pp. 324.

35 . Résolution 1617 (2005), résolution 1720 (2006), résolution 1735 (2006) et résolution 1822 (2008).

36 . United Nations General Assembly - Security Council, *Enclosure: Improving the Implementation of Sanctions Regimes Through Ensuring "Fair and Clear Procedures"*, New York, 2 juillet 2008.

nuent d'achopper sur le type de mécanisme révisionnel approprié, des membres du Conseil de sécurité (à commencer par les cinq permanents) arguant du caractère administratif et préventif de la liste pour la placer au-dessus de toute révision judiciaire [37].

A cette conflictualité médiatisée [38] autour de la révision des listes, du droit d'être entendu et de pouvoir bénéficier d'un contrôle juridictionnel effectif, se superpose logiquement celle concernant les difficultés éprouvées pour ne plus être répertorié sur les « listes noires ». En effet, un retrait de la liste ONU requiert un consentement unanime du Conseil de sécurité. Le dévoilement critique des implications de cet état de fait a été relayé par la médiation d'articles de presse relatant le parcours de « victimes collatérales » de la lutte antiterroriste. Parmi les récits d'« innocents accusés à tort », il convient d'évoquer le cas symbolique de Nabil Sayadi et Patricia Vinck qui a été particulièrement commenté par la presse belge et française [39]. Ce couple belge a officiellement été enregistré le 23 janvier 2003 par le « comité 1267 » suite à l'ouverture d'une instruction judiciaire entamée en Belgique le 3 septembre 2002 et à des informations transmises à ce comité par l'Etat belge le 19 novembre 2002. Le 11 février 2005, la procédure judiciaire aboutit au jugement du tribunal de première instance de Bruxelles enjoignant l'Etat belge d'initier une demande de radiation auprès du comité de sanctions des Nations unies. Le 19 décembre 2005, ce même tribunal confirmera l'innocence des prévenus en prononçant un non-lieu. Pour autant, si l'Etat belge a bien sollicité le « comité 1267 » pour délister ses nationaux, aucune décision ne viendra alors valider cette requête. Evoquant l'idée de « mort civile [40] » engendrée par le gel de leurs avoirs, l'at-

37 . Cf. Lopez G. A., Cortright D., Millar A., Gerber-Stellingwerf L., *Overdue Process: Protecting Human Rights while Sanctioning Alleged Terrorists* (A report to Cordaid from the Fourth Freedom Forum and Kroc Institute for International Peace Studies at the University of Notre Dame), avril 2009.

38 . *The Washington Post*, "Terrorism Financing Blacklists at Risk", 2 novembre 2008.

39 . A titre d'exemples : *La libre Belgique*, « Affaire Sayadi-Vinck : le troisième essai », 19 décembre 2008 ; « Plainte à Genève contre la Belgique », 1er juin 2006 ; *Le Monde*, « Un couple belge dans l'enfer de la lutte anti-terroriste », 3 juin 2006 ; « Inscrit sur la liste antiterroriste de l'ONU, un couple belge, innocenté, est réduit à une "mort civile" », 24 décembre 2008 ; *Le Soir*, « Deux belges figés sur la liste des sympathisants d'Al-Qaida », 12 septembre 2003 ; « La commission 11 septembre ne peut rien prouver - Al-Qaida : deux belges "innocentés" », 26 août 2004 ; « Radier deux belges de la liste des terroristes - les Sayadi-Vinck réhabilités », 24 février 2005 ; « Nabil Sayadi et Patricia Vinck », 23 décembre 2008 ; « L'ONU les retire d'une liste de "terroristes" : Sayadi et Vinck sont enfin réhabilités », 23 juillet 2009 ; « Nabil Sayadi mis au ban de la société pendant six ans : "On nous appelait Ben Laden" », 24 juillet 2009.

40 . Cette rhétorique de « mort civile » est également employée par d'autres, comme Jose Maria Sison, ressortissant philippin inscrit sur la liste autonome de l'UE le 22 octobre 2002, pour matérialiser les implications de l'« injustice » dont ils considèrent être frappés, espérant ainsi mobiliser autour de leur « cause ». Entretien avec Jose Maria Sison, Utrecht, juin 2009 ; entretien téléphonique avec Georges-Henri Beauthier (avocat de Nabil Sayadi et Patricia Vinck), juin 2009. Cf. aussi The International DEFEND Committee, *European Court to hear Sison complaint against terrorist blacklist of EU Council*, 28 avril 2009 ; www.josemariasison.org. Suite à l'arrêt du tribunal de première instance des communautés européennes du 30 septembre 2009, le nom de M. Sison a finalement été retiré de la liste autonome telle que révisée le 22 décembre 2009. Voir Arrêt du tribunal de première instance dans l'affaire T-341/07, *Jose Maria Sison contre Conseil*, communiqué de presse Commission européenne service juri-

teinte à leur réputation et la privation de passeport, de travail et de revenus, les plaignants – par la voix de leur avocat – finiront par saisir le Comité des droits de l'homme de l'ONU en mars 2007. Le 22 octobre 2008, celui-ci a rendu un avis très critique envers l'attitude de l'Etat belge, estimant qu'il avait le « *devoir de faire tout ce qu'il peut pour retirer les deux noms de la liste dès que possible* [41] ». En conséquence de quoi, la Belgique a émis une troisième demande de radiation qui a finalement débouché, le 21 juillet 2009, sur la réhabilitation des deux personnes après six ans d'inscription et de mesures restrictives dites temporaires. Ce dénouement reste de l'ordre de l'exception puisque, pour l'année 2008, le « comité 1267 » a ajouté 32 entités aux 500 déjà listées et en a retiré trois, dont une pour cause de décès [42]. Toujours est-il qu'en référence à nombre de cas individuels subsumés sous une même catégorie, une cause a émergé – la dénonciation des mécanismes d'inclusion et d'exclusion des « listes noires » –, portée par un ensemble d'acteurs critiques différents faisant appel au respect des droits fondamentaux. La clarté avec laquelle l'enjeu des listes vient à être porté par ces multiples « dénonciateurs », formant un espace public large, tranche avec les mises en accusation ayant émergé dans les deux autres cas de figure étudiés de la lutte contre l'argent sale.

SWIFT : une affaire sans résonance

SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) se présente comme une entreprise « *par l'intermédiaire de laquelle le secteur des finances effectue ses transactions financières avec rapidité, assurance et en toute confiance* [43] ». Le rôle de cette société coopérative (créée en 1973 par 239 banques de 15 pays dont le siège social est situé à la Hulpe, en Belgique) se conçoit ainsi comme celui de fournisseur, mondialement dominant, de messageries automatisées permettant aux organismes clients d'échanger des informations financières standardisées. Plus de 8 000 clients professionnels (institutions financières pour l'essentiel) ont recours à la palette de services proposés par SWIFT afin de réaliser des transferts monétaires, et ce dans plus de 200 pays. En 2009, une moyenne de 14,6 millions de messages financiers transitent quotidiennement par le service SWIFTN et FIN pour un total de près de 3,9 milliards de messages sur l'année précédente. L'utilisation de traitements automatisés pour les flux internationaux de capitaux sous-entend *in fine* « *l'importance systémique de SWIFT pour le système global des paiements* [44] ». Sans qu'elle ne soit véritablement dans une situation monopolistique, cette

dique, novembre 2009 ; Council of the European Union, *Review of the EU autonomous regime on measures to combat terrorism*, 22 décember 2009.

41 . United Nations - Human Rights Committee, *Communication No. 1472/2006 : Nabil Sayadi and Patricia Vinck/Belgium on Application to have names removed from the Consolidated List of the United Nations Sanctions Committee*, 22 octobre 2008.

42 . Lopez et *al.*, *Overdue Process : Protecting Human Rights while Sanctioning Alleged Terrorists*, *op.cit.*.

43 . www.swift.com

44 . Banque Nationale de Belgique, *Financial Stability Review 2005. Synthèse*, juin 2005, p. 14.

société a donc acquis une position cruciale dans le fonctionnement du système financier global en tant que messager facilitant les transactions entre établissements bancaires notamment. Un usage détourné de son rôle d'intermédiaire et de pivot du système des paiements va valoir à cette entreprise d'être publiquement mise en accusation dans ce qui va devenir, au cours de l'année 2006, l'« affaire SWIFT ».

Dévoilement et « retournement d'accusation »

Le 23 juin 2006, le *New York Times* entreprend de dévoiler l'existence d'un programme confidentiel de surveillance financière initié par le gouvernement américain au lendemain des événements du 11 septembre 2001 [45]. Pointant les abus susceptibles de résulter de l'ampleur de ce programme, le long article révèle en particulier la place prépondérante de SWIFT dans ce scandale. Depuis plus de quatre ans, les autorités américaines ont secrètement eu accès aux messages transitant par le « *centre nerveux de l'industrie bancaire mondiale* [46] » afin de tracer les transactions financières d'individus suspectés de terrorisme. Ce quotidien ayant visiblement pris sur lui la responsabilité d'être le « lanceur d'alerte [47] », d'autres journaux décident de lui emboîter le pas et publient au même moment l'information selon laquelle SWIFT a transféré aux autorités les copies de messages interbancaires du monde entier [48]. Le même jour, deux avocats américains lancent une action en justice afin d'intenter un procès à l'entreprise pour violation de leurs droits au respect de la vie privée [49]. Une fois ouvert, le contenu d'un message SWIFT relatif au paiement d'un client d'une banque comprend en effet des données personnelles telles que les noms du bénéficiaire et du commanditaire de la transaction financière, leur adresse, leur numéro d'identification nationale ainsi que d'autres informations relatives au message financier.

Les réactions et rapports qui suivront cette mise en visibilité apporteront des compléments d'information et quelques corrections mais confirmeront la majeure partie des faits exposés sur l'existence du *Terrorist Finance Tracking Program*. Ce programme a débuté presque immédiatement après le 11 septembre 2001 et l'emploi de l'adjectif « secret » pour le qualifier ne semble pas excessif puisque l'accord du Congrès américain n'a pas été un préalable à son

45 . *The New York Times*, "Bank data sifted in secret by U.S. to block terror", 23 juin 2006.
46 . *Ibid.*
47 . Sur la notion de lanceur d'alerte, cf. Chateauraynaud F., Torny D., *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, Editions de l'Ecole des hautes études en sciences sociales, 1999.
48 . *The Los Angeles Times*, "Secret U.S. Program Tracks Global Bank Transfers", 23 juin 2006 ; *The Washington Post*, "Bank Records Secretly Tapped: Administration Began Using Global Database Shortly After 2001 Attacks", 23 juin 2006 ; *The Wall Street Journal*, "U.S. Treasury Tracks Financial Data in Secret Program", 23 juin 2006.
49 . Cité dans Köppel J., "The Swift Affair: Swiss Banking Secrecy and the Fight against Terrorist Financing", Graduate Institute of International and Development Studies, unpublished paper, 2009, pp. 16-17.

application. Pour ce faire, l'OFAC (*Office of Foreign Assets Control*), une division du Trésor, a justifié son action en référence à des mandats statutaires américains [50] et au fameux décret présidentiel 13224 autorisant le département du Trésor – en coordination avec d'autres agences fédérales – à « *utiliser toutes mesures appropriées pour identifier, traquer et poursuivre* » les groupes terroristes et leurs soutiens [51]. Sur cette base légale, l'OFAC s'est donc contentée d'adresser des injonctions administratives (*subpoenas*) contraignant systématiquement SWIFT à extraire et transmettre la copie de messages demandés selon des critères communs (dates et pays principalement). Mais au-delà d'un simple exercice de justification de la légalité et de la valeur ajoutée de son programme, l'administration Bush a surtout vigoureusement déploré l'attitude de la presse, la stigmatisant comme une atteinte inexcusable à la sécurité nationale. Cette posture extrêmement critique ne va cesser de s'amplifier dans les jours suivant les révélations du *New York Times*, ce qui va donner lieu à un véritable « *retournement de l'accusation scandaleuse en direction de l'accusateur* [52] ».

Rapidement, ce n'est plus le programme de surveillance généralisée qui est mis en cause, mais l'acte public qui l'a révélé : le scandale initial n'ayant été qu'une brève séquence d'ouverture à ce qui va se transformer en « affaire SWIFT » [53]. Le républicain Peter T. King (président du *House Homeland Security Committee*) va jusqu'à demander formellement le début d'une enquête et des poursuites pénales contre le *New York Times*, l'accusant de « traîtrise » en temps de guerre [54]. Bien que d'autres hommes politiques ne partagent pas ce point de vue [55], la virulence des réactions politiques – mais aussi d'une partie de la population – pousse finalement Byron Calame (médiateur du journal new-yorkais) à justifier la publication de l'article. Dans une tribune datée du 2 juillet 2006, celui-ci relativise tout d'abord la nature secrète du programme de surveillance en soulignant notamment qu'il en était fait mention, dès 2002, dans un rapport public des Nations unies [56]. Reconnaissant

50 . Mention est faite de *The International Emergency Economic Powers Act of 1977* ; *The United Nations Participation Act*.

51 . Cf. U.S. Department of the Treasury, *Terrorist Finance Tracking Program: Fact Sheet*, 23 juin 2006.

52 . De Blic D., Lemieux C., « Le scandale comme épreuve : éléments de sociologie pragmatique », *op.cit.*, p. 17.

53 . Sur le jeu de transformation des scandales en affaires, cf. Lemieux C., « L'accusation tolérante : remarques sur les rapports entre commérage, scandale et affaire » in Boltanski L., Claverie E., Offenstadt N., Van Damme S. (dir.), *Affaires, scandales et grandes causes. De Socrate à Pinochet*, Paris, Stock, 2007, pp. 367-369.

54 . *The Washington Post*, "Lawmaker Wants Times Prosecuted", 26 juin 2006.

55 . Arlen Specter (président du comité judiciaire du Sénat) considère par exemple que : « *Sur la base de l'article du journal, je pense qu'il est prématuré d'appeler à la poursuite du New York Times, tout comme je pense qu'il est prématuré de dire que l'administration a entièrement raison* ». Cité dans *The Washington Post*, *ibid.*

56 . *The New York Times*, "Secrecy, Security, the President and the Press", 2 juillet 2006. Le rapport évoqué sans plus de références étant : Conseil de Sécurité, *Troisième rapport du Groupe de suivi en application du paragraphe 10 de la résolution 1390*, 17 décembre 2002, point 31, p. 12.

ensuite que la discrétion est certes un élément vital des opérations de renseignement, mais qu'elle n'exclut pas leur suivi par les législateurs élus, il considère que la faible supervision du Congrès motivait l'examen public d'une mesure temporaire d'urgence devenue permanente [57]. Malgré cela, la controverse publique pressera finalement Byron Calame à faire son *mea culpa* quelques mois plus tard, à regretter la publication de cet article et à reconnaître l'apparente légalité du *Terrorist Finance Tracking Program* ainsi que l'absence de preuves démontrant un usage abusif des données personnelles collectées [58]. Enfin, en octobre 2007, les deux avocats sont déboutés de leur action en justice entamée le 23 juin 2006, le juge ayant estimé que les plaignants n'avaient apporté aucune preuve étayant le fait que leurs données personnelles avaient été directement visées par le *Terrorist Finance Tracking Program* [59]. Le gouvernement fédéral avait de toute façon pris les devants en annonçant, en août 2007, qu'il invoquerait l'outil juridique du *State Secret Privilege* pour stopper toute poursuite contre SWIFT [60].

Une affaire transatlantique

Outre cet aspect exclusivement américain, l'affaire SWIFT est aussi et surtout marquée par sa dimension transatlantique. Les révélations sur le programme de surveillance financière ont eu un écho tout particulier en Europe, où une partie de la sphère médiatique n'a pas tardé à les relayer [61] en questionnant la collaboration entre SWIFT et le Trésor américain à l'aune de la législation européenne sur la protection des données à caractère personnel. Etablie en Belgique, la société coopérative est effectivement soumise au droit européen. Se référant à ces enquêtes journalistiques et à une plainte déposée par l'organisation *Privacy International* [62], le Parlement européen adopte une résolution à ce sujet le 6 juillet 2006, soit moins de 15 jours après la divulgation des premières informations. Les parlementaires expriment alors leur regret d'avoir été maintenus dans l'ignorance et s'inquiètent de la « *création d'un climat marqué par la dégradation du respect de la vie privée et de la protection des données* [63] ». Etant donné l'importance capitale du réseau SWIFT

57 . *The New York Times*, "Secrecy, Security, the President and the Press", 2 juillet 2006.
58 . *The New York Times*, "Banking Data: A Mea Culpa", 22 octobre 2006.
59 . District Court for the Eastern District of Virginia, *Ian Walker and Stephen Kruse, Plaintiffs, v. S.W.I.F.T. SCRL, Defendant*, 517F. Supp. 2d 801, 2007, p. 517-525v ; cité dans Köppel 2009.
60 . *The New York Times*, "U.S. Cites «Secrets» Privilege as It Tries to Stop Suit on Banking Records", 31 août 2007.
61 . *The Guardian*, "Bush under fire over tracking of money transfers", 23 juin 2006 ; *Le Monde*, « La CIA a espionné les flux bancaires internationaux », 25 juin 2006 ; *Le Soir*, « Les intrusions de la CIA dans les données confidentielles », 26 juin 2006.
62 . Dès juin 2006, cette association de défense des droits de l'Homme spécialisée dans l'observation des pratiques de surveillance des gouvernements et des entreprises, a déposé plainte auprès des instances de contrôle de la protection des données et de la vie privée dans 33 pays. Voir www.privacyinternational.org
63 . Parlement européen, *Résolution du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains*, Strasbourg, 6 juillet

pour les banques européennes, sa mise sous surveillance annonce l'accès massif des autorités américaines à des informations confidentielles relatives à des millions de citoyens européens sans l'accord des institutions de l'UE. Le texte de la résolution insiste d'ailleurs sur la question de la souveraineté économique, dénonçant le danger – au moins théorique – d'espionnage économique et industriel à grande échelle qui résulte de la communication non contrôlée de ces données à un pays tiers, en l'occurrence les Etats-Unis.

Ayant été saisies pour avis, les autorités belges et européennes de protection des données font de cette affaire une priorité. En septembre 2006, la Commission belge de la protection de la vie privée est la première à rendre un avis dont la problématique est centrée sur le rôle joué par SWIFT lors de la transmission de données à caractère personnel au département du Trésor américain. Sa conclusion est exempte de toute ambiguïté : les pratiques secrètes, massives, systématiques et de longue durée de l'entreprise vis-à-vis de l'OFAC constituent une violation de principes fondamentaux dans l'ordre juridique européen [64]. Une audition publique est ensuite organisée au début du mois d'octobre 2006 par le Parlement européen : elle donne l'occasion à Francis Vanbever (alors directeur financier de SWIFT) de présenter la position de la compagnie. Celle-ci rejette l'avis de l'autorité belge et, arguant de son statut juridique spécifique et des limitations négociées avec le Trésor, récuse toute infraction à la législation européenne. Se posant en victime d'un conflit juridique et s'estimant prise en étau entre les lois belges de protection des données et les lois antiterroristes américaines, la société SWIFT réitère son appel à un dialogue transatlantique sur ces enjeux. Nonobstant cette posture de victime de formes juridiques concurrentes, les avis ultérieurs du groupe de l'« article 29 » (G 29) [65] et du Contrôleur européen de la protection des données (CEPD) [66] ne diffèrent pourtant pas du précédent belge. Issue d'un travail concerté, l'opinion du G 29 confirme les infractions et condamne le contournement des « *mécanismes existants permettant le contrôle indépendant du traitement des données* » financières provenant d'une entreprise ayant son

2006. Une deuxième résolution sera adoptée en février 2007, cf. Parlement européen, *Résolution du Parlement européen sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions*, 14 février 2007.

64 . Commission de la protection de la vie privée (Royaume de Belgique), *Avis n°37 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC)*, 27 septembre 2006.

65 . Institué par l'article 29 de la directive européenne de 1995 sur la protection des données, ce groupe de travail rassemble les représentants de chaque autorité indépendante nationale de protection des données des Etats-membres. La mission confiée au G 29 consiste à contribuer à l'élaboration des normes européennes en adoptant des recommandations, en rendant des avis sur le niveau de protection dans les pays tiers et en conseillant la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles.

66 . La fonction de Contrôleur européen à la protection des données a été créée par le Règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation des données. Institution indépendante, elle a surtout pour objectif de contrôler les traitements de données à caractère personnel effectués par l'administration de l'UE.

siège au sein de l'UE [67]. Jugeant cet usage sécuritaire disproportionné et incompatible avec la finalité commerciale originale du traitement des données SWIFT, il estime que cet abus est susceptible d'avoir des répercussions directes sur la vie des individus dont les données sont concernées. Également mises en cause, les institutions financières européennes – utilisatrices du service SWIFTNet Fin – sont sommées d'informer leurs clients particuliers sur le devenir de leurs données personnelles et l'éventuel accès des autorités américaines à ces renseignements. Ce qu'elles feront majoritairement par le biais d'un encadré inséré sur leur site Internet. En février 2007, le CEPD vient réaffirmer les avis de la Commission belge et du G29, en se focalisant toutefois plus particulièrement sur le rôle joué par la Banque centrale européenne (BCE) dans l'affaire SWIFT et en lui reprochant vivement son silence. En effet, la BCE fait partie du groupe des dix banques centrales supervisant les activités de la société coopérative et, à ce titre, elle a pris connaissance du *Terrorist Finance Tracking Program* dès 2002 [68]. Toutefois, selon cette institution, les règles de confidentialité et le champ d'action limité inhérents à sa fonction de supervision ne lui permettaient pas de relayer l'information auprès des autorités européennes de protection des données, ni de faire pression sur SWIFT dans ce sens (ce que contestera l'avis des dites autorités [69]).

Bien plus qu'une simple affaire juridique et technique, le cas SWIFT se double d'une dimension politique indéniable. Ayant appris l'existence du programme de surveillance par voie de presse, le Parlement européen mais aussi la Commission européenne l'ont ressenti comme un profond choc politique, accentué par le mutisme avéré de certaines institutions telles que la BCE [70]. Dans un deuxième avis de décembre 2006, la commission belge de la protection de la vie privée exhortera d'ailleurs les gouvernements européens à ne pas rester silencieux devant un « *motif de protestation justifié* [71] ». Néanmoins, l'unanimisme critique des autorités de protection des données se heurtera à l'indifférence apparente des Etats membres. En lieu et place d'une condamnation diplomatique, certains d'entre eux – dont la France et le Royaume-Uni – s'empresseront au contraire d'attester, devant le Conseil de l'UE, de la véra-

67 . Groupe de travail « Article 29 » 2006.

68 . Menant les opérations de supervision de SWIFT, le G 10 se compose de la Banque nationale de Belgique, la Banque du Canada, la Banque d'Allemagne, la Banque centrale européenne, la Banque de France, la Banque d'Italie, la Banque du Japon, la Banque des Pays-Bas, la Banque de Suède, la Banque nationale suisse, la Banque d'Angleterre et la Réserve fédérale des Etats-Unis.

69 . Contrôleur européen de la protection des données, *Avis du CEPD sur le rôle de la Banque centrale européenne dans l'affaire SWIFT*, février 2007.

70 . Entretien avec des officiels de la Commission européenne, Bruxelles, décembre 2007 et mai 2008.

71 . « *Le constat que, durant des années, des données à caractère personnel de leurs citoyens aient fait l'objet, à grande échelle, d'une enquête jusqu'à nouvel ordre incontrôlée et unilatérale par les autorités d'un Etat avec lequel une collaboration étroite a lieu constitue en soi un motif de protestation justifié* », Commission de la protection de la vie privée (Royaume de Belgique), *Avis relatif à la préparation d'un convention concernant la transmission de données à caractère personnel par SWIFT à l'US Department of the Treasury (UST)*, 20 décembre 2006.

cité des affirmations américaines sur l'utilité du programme pour lutter contre le terrorisme, y compris en Europe [72]. Les services de renseignements de certains États-membres ont effectivement reçu des informations issues du *Terrorist Finance Tracking Program* via des relations bilatérales informelles [73].

Parallèlement à cette ambivalence des gouvernements européens, les « propositions d'engagement » des autorités de protection des données pâtissent plus généralement d'un manque de réactions collectives qui tend à relativiser les fautes dénoncées. Passées les premières révélations, l'attention accordée dans l'UE à l'affaire SWIFT retombe médiatiquement en quelques jours avec une absence relative de mobilisation. Aucune procédure judiciaire n'est engagée. L'affaire ne franchit pas vraiment les frontières des institutions européennes et demeure extrêmement sectorisée, la critique restant cantonnée au périmètre des professionnels de la protection des données. Ce qui pourrait ressembler de près ou de loin à l'émergence d'une cause n'apparaît donc pas car l'action de ces professionnels ne débouche aucunement sur la constitution d'une force de dénonciation plus importante. Finalement, cette affaire aboutit assez discrètement, en juin 2007, à un accord transatlantique aux contours inhabituels puisqu'il se présente sous la forme d'engagements unilatéraux des Etats-Unis concernant le traitement des données SWIFT [74]. Ces observations unilatérales sont accompagnées d'un échange de lettres formelles entre le département du Trésor américain et la Commission ainsi que le conseil de l'UE [75]. La mise en conformité des transferts SWIFT par rapport à la législation européenne y est saluée.

Enfin, l'avis définitif (décembre 2008) de la Commission belge de protection de la vie privée a semblé marquer le point final d'une affaire sans caisse de résonance. Cette Commission a prolongé durant deux années ses investigations, marquant un virage à 180 degrés au regard de ses premières positions de 2006 [76]. Toute idée de poursuites contre la société coopérative est abandonnée puisque la décision conclut à la légalité du programme de surveillance et à la protection adéquate dont ont bénéficié les communications de données effectuées par SWIFT [77]. L'autorité belge justifie en partie ce renversement par

72 . Entretien avec des officiels de la Commission européenne, Bruxelles, décembre 2007.

73 . Comme l'a indiqué Gilles de Kerchove (coordinateur européen de la lutte contre le terrorisme) lors d'une conférence publique. *Challenge International Conference: The Exchange and Storage of Data*, Sciences Po, Paris, 10-11 octobre 2008.

74 . Département du Trésor des Etats-Unis, *Programme de surveillance du financement du terrorisme - Observations du Département du Trésor des États-Unis*, *J.O.* de l'UE, 2007/C 166/09, (Traduction) 20 juillet 2007.

75 . Levey S., *Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Programme*, *Official Journal of the European Union*, 2007/ C 166/08, 28 juin 2007 ; Frattini F., Steinbrück P., *Réponse de l'UE au département du Trésor des États-Unis - SWIFT/programme de surveillance du financement du terrorisme*, *J.O.* de l'UE, 2007/C 166/10, 20 juillet 2007.

76 . Commission de protection de la vie privée (Royaume de Belgique), *Contrôle et procédure de recommandation initiés à l'égard de la société SWIFT scrl*, décision du 9 décembre 2008.

77 . *Ibid.*, p. 76.

l'appréciation de faits alors mal connus, même si ce sont surtout les efforts consentis par SWIFT depuis 2006 qui soutiennent implicitement cette décision *a priori* surprenante [78]. En cela, le présent avis ne fait d'ailleurs qu'entériner l'opinion émise par ses pairs européens à partir d'octobre 2007. Sous pression après la mise en visibilité du programme de surveillance, l'entreprise n'a jamais cédé sur le fond de son discours défensif mais s'est résignée, en pratique, à modifier l'architecture technique de son réseau afin de protéger sa réputation [79]. Dès la fin de l'année 2007, ces changements ont été accueillis très favorablement par les institutions de protection des données qui, revendiquant d'en être à l'origine, ont parlé de « sortie de crise [80] ». La restructuration de l'architecture de messagerie SWIFT se résume à l'implantation d'un nouveau centre opérationnel en Suisse (prévu pour fin 2009) afin que les données des messages relatifs aux transactions intra-européennes restent désormais en Europe. Autrement dit, la surveillance américaine concernerait uniquement les messages en provenance ou à destination des États-Unis et non plus ceux émis entre des clients présents sur le continent européen. L'affaire a donc tout de même conduit à des transformations de fonctionnement.

Cette condition *sine qua non* de l'approbation des autorités précitées mérite toutefois l'usage du conditionnel, voire du passé composé, au vu des négociations informelles transatlantiques menées en 2009 afin de perpétuer l'accès des Etats-Unis aux informations bancaires de citoyens européens transitant par SWIFT [81]. Le dévoilement d'un nouvel accord en préparation a rencontré l'indignation des mêmes médiateurs critiques (Parlement européen et autorités de protection des données) [82]. En juillet 2009, le Conseil de l'Union européenne a ainsi donné mandat à sa présidence suédoise et à la Commission pour parvenir à un accord remanié. La tenue de ces négociations avait dès lors pour finalité d'anticiper la relocalisation effective des centres opérationnels de l'entreprise belge. Apprenant une nouvelle fois l'existence de ce projet par voie de presse, des parlementaires n'ont pas manqué de s'en plaindre auprès de la Commission. Cela s'est traduit par l'adoption d'une nouvelle résolution destinée à rappeler les conditions jugées nécessaires afin d'assurer le respect de la vie privée et de la protection des données [83]. Renouvelant leurs craintes sur le danger potentiel d'espionnage économique et industriel, les députés ont

78 . Pour une interprétation de la stratégie des autorités de protection des données, cf. Köppel J., "The Swift Affair: Swiss Banking Secrecy and the Fight against Terrorist Financing", *op.cit.*.

79 . « SWIFT. Le Conseil d'administration de SWIFT approuve la nouvelle architecture de messagerie », communiqué SWIFT, Bruxelles, le 4 octobre 2007.

80 . Groupe de travail « Article 29 », Data Protection Working Party, *Press release 62nd session*, 11 octobre 2007, p. 1 ; CNIL, *28e rapport d'activité*, Paris, La Documentation française 2007, pp. 23-24.

81 . Entretien avec un conseiller à la représentation permanente d'un Etat-membre de l'UE, mai 2009.

82 . *European Voice*, "Commission to seek new deal with the US on data transfers", 16 juillet 2009 ; *Le Temps*, « Les Etats-Unis obtiendraient l'accès aux données de Swift via la Suisse », 22 juillet 2009 ; *EU Observer*, "EU bank data move ignored legal advice", 29 juillet 2009.

83 . Parlement européen, *Résolution du Parlement européen sur l'accord international envisagé pour mettre à la disposition du département du Trésor des États-Unis des données de message-*

également sollicité un certain nombre de garanties minimales telles qu'un mécanisme de réciprocité « *obligeant les autorités compétentes des Etats-Unis à communiquer aux autorités compétentes de l'Union, sur demande, les données de messagerie financière pertinentes* ». Contrairement au Parlement, le contrôleur européen de protection des données a bien été consulté par la Commission en juillet 2009, ce qui lui a permis d'émettre des doutes sur la base légale de l'accord [84]. Enfin, le Conseil de l'UE a rencontré des difficultés pour dégager en son sein une position unanime, l'Allemagne et l'Autriche ayant exprimé des réserves vis-à-vis du niveau de protection des données consenti [85].

Les gouvernements européens ont tout de même fini (les deux Etats membres réfractaires s'étant abstenus lors du vote au Conseil) par conclure un nouvel accord avec les autorités américaines le 30 novembre 2009, soit un jour avant l'entrée en vigueur du traité de Lisbonne élargissant significativement les prérogatives du Parlement européen sur ce type d'accord international. Néanmoins, cette décision a finalement été limitée à un engagement intérimaire officiellement justifié pour prévenir toute rupture temporaire de transferts de données, amenées à être stockées dans le nouveau serveur SWIFT, en direction des Etats-Unis. Le Conseil a ainsi réaffirmé la légalité de cette conciliation intérimaire et l'utilité du *Terrorist Finance Tracking Program* pour la sécurité européenne, et ce tout en notifiant qu'un accord transatlantique définitif serait négocié d'ici la fin de l'année 2010 avec la participation du Parlement. Un discours d'apaisement qui n'a pas convaincu l'ensemble de ses destinataires puisque la Commission parlementaire des libertés civiles (LIBE) a adopté, le 5 février 2010, un texte appelant à rejeter les termes de l'accord transitoire [86]. Discutée en assemblée plénière, cette position a été approuvée par le Parlement européen le 11 février, par 378 voix contre 196 et 31 abstentions. Entré formellement en vigueur 11 jours plus tôt et désormais invalidé, l'accord fait ainsi les frais de la toute première utilisation du droit de veto attribué au Parlement par le traité de Lisbonne. Les arguments émanant de la Commission et du Conseil, faisant état d'un « vide de sécurité » (*security gap*) en cas de rejet [87], n'auront donc pas suffi, le rapporteur du Parlement réitérant les inquiétudes en matière de protection des données et de recours judiciaire tout en regrettant que l'UE « *continue à externaliser ses services de sécurité aux*

rie financière afin de prévenir et de combattre le terrorisme et le financement du terrorisme, 17 septembre 2009.

84 . Parlement européen, *Joint meeting of LIBE and ECON Committees on EU-US interim agreement following the entry into force of the new SWIFT architecture: Peter Hustinx, European Data Protection Supervisor, speaking points*, 3 septembre 2009.

85 . *European Voice*, "Pressure grows on opponents of bank transfer data deal", 26 novembre 2009.

86 . Parlement européen, Service de presse, *SWIFT, les données bancaires des européens traverseront-elles l'Atlantique ?*, 5 février 2010.

87 . A titre d'exemples : Conseil de l'Union européenne, *EU-US Agreement on the Transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Programme*, 9 février 2010.

Etats-Unis sans réciprocité [88] ». L'affaire SWIFT tend ainsi à se poursuivre et à se polariser autour d'un affrontement institutionnel européen auquel vient s'ajouter une pression américaine de plus en plus visible [89]. Reste à savoir si l'engagement des médiateurs critiques arrivera à créer un espace public (partageant un même sentiment d'indignation en dehors de leur périmètre institutionnel) articulé autour de la thématique de la « perte de contrôle problématique de la protection des données personnelles [financières] une fois qu'elles ont quitté la juridiction européenne [90] ». Le prochain épisode pourrait d'ailleurs être l'examen de la possibilité d'un *EU Terrorist Tracking Financial Programme* à en croire le coordinateur européen de la lutte antiterroriste [91].

Si la possibilité d'existence d'une mobilisation multisectorielle semble être à relativiser sur cet exemple d'accès à des bases de données commerciales pour des motifs sécuritaires, ce surgissement critique apparaît bien plus improbable encore concernant les pratiques bancaires de surveillance, tant les formes d'appel à l'« opinion » restent inaudibles.

La boîte noire : l'usage bancaire des technologies de surveillance

Mises en œuvre par les banques conformément à leurs obligations dans le cadre de la lutte contre l'argent sale, les pratiques de détection des transactions suspectes ne suscitent guère d'intérêt du point de vue des atteintes aux libertés fondamentales. C'est pourtant au niveau des établissements financiers privés que s'opère quotidiennement ce combat. Soumises à des injonctions gouvernementales de plus en plus contraignantes, notamment depuis les événements du 11 septembre, les banques ont dû en effet assumer leurs responsabilités en élaborant des dispositifs sophistiqués de gestion des risques liés au blanchiment et au financement du terrorisme [92]. De tels dispositifs comprennent en particulier l'usage routinisé d'outils informatiques spécialisés, dont le marché n'a cessé de s'étendre au cours des années 2000 [93]. La principale motivation des établissements bancaires a beau être liée à un souci d'auditabilité [94] – afin de se

88 . Parlement européen, Service de presse, *SWIFT : les députés rejettent l'accord et protègent les données*, 11 février 2010.

89 . Des eurodéputés ont jugé très inhabituelles les pressions des autorités américaines sur leur institution, relevant notamment l'appel téléphonique de la secrétaire d'Etat américaine Hillary Clinton au président du Parlement européen Jerzy Buzek, avant le vote de la Commission LIBE. Voir par exemple la vidéo *Accord SWIFT: Enjeux, procédure et réactions* par europarltv.

90 . Fuster G. G., De Hert P., Gutwirth S., "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology*, vol. 22, n°1-2, 2008, pp. 191-202.

91 . Conseil de l'Union européenne, *Note from EU Counter-Terrorism Coordinator to Council/European Council: European Counter-Terrorism Strategy – Discussion paper*, 26 novembre 2009.

92 . Sur la montée en puissance d'une approche fondée sur la gestion des risques, cf. Hood C. Rothstein H., Baldwin R., *The Government of Risk. Understanding Risk Regulation Regimes*, Oxford, Oxford University Press, 2001 ; Levi M., Wall D. S., "Technologies, Security and Privacy in post-9/11 European Information Society", *Journal of Law and Society*, vol. 31, n° 2, 2004, pp. 194-220

prémunir contre toute mise en cause de la part des autorités régulatrices gouvernementales en arguant du respect de procédures scrupuleuses – il reste que ces outils aident les professionnels à forger leurs soupçons. De plus, ces instruments traitent des informations pouvant constituer des renseignements économiques et servir, à ce titre, de monnaie d'échange dans les interactions que les personnels en charge de l'anti-blanchiment dans les banques nouent de manière croissante avec les services policiers et de renseignements compétents. La routinisation des relations entre ces univers professionnels qui s'ignoraient il y a peu encore est d'ailleurs le principal aboutissement de deux décennies d'offensives globales contre l'argent sale [95].

Filtrage et profilage

Les outils informatiques tendent à offrir aujourd'hui un ensemble de fonctionnalités qui, auparavant, étaient vendues de manière distincte. Ils permettent en premier lieu de réaliser des opérations de filtrage liées au développement des « listes noires » dans la lutte contre les délinquances transnationales. En effet, ces listes ne se limitent pas aux personnes et aux organisations suspectées de lien avec des activités terroristes, déjà mentionnées dans la première partie de cet article. Les banques sont également tenues de prendre garde aux relations qu'elles sont susceptibles de développer avec les « personnes politiquement exposées » (PPE). Figurant dans les recommandations du GAFI révisées en 2003 [96] et dans la troisième directive antiblanchiment de l'UE [97], cette notion ambiguë désigne l'ensemble des responsables politiques (chefs d'Etat, ministres, chefs de partis, directeurs de grandes entreprises d'Etat, leaders régionaux et municipaux) et leur entourage. Toutes les juridictions sont en principe concernées, sauf celles d'Europe car la définition européenne des PPE exclut les Etats membres de l'UE. Les producteurs d'outils informatiques ont répondu à cette nouvelle demande en élaborant des systèmes de collecte et de traitement d'informations sur cette population, à partir de sources publiques. Souvent associés à des agences de presse, ils revendiquent de détenir des informations sur près d'un demi-million d'individus [98]. De leur côté, les banques prennent fréquemment l'initiative d'ajouter à ces listes des informations qu'elles jugent pertinentes, à l'instar du classement annuel de *Transparency International* ou de l'appréciation des pays sensibles au risque drogue de l'ONU [99]. La considération accordée aux territoires dans lesquels se déroulent les transactions culmine avec la prise en compte des

93 . Pour une grande banque française, l'équipement au milieu des années 2000 a pu coûter plusieurs dizaines de millions d'euros.

94 . Favarel-Garrigues G., Godefroy T., Lascoumes P., *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, *op.cit.*, pp. 210-217.

95 . *Ibid.*, pp. 237-258.

96 . Voir la recommandation n° 6 : http://www.fatf-gafi.org/dataoecd/8/44/33664453.PDF

97 . UE, « Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme », *JO*, L309 du 25 novembre 2005.

98 . Voir par exemple le site Internet de *World-Check* : http://www.world-check.com/

embargos. Actuellement le plus emblématique, le cas de l'Iran illustre une nouvelle priorité accordée à la répression du financement de la prolifération nucléaire dans les institutions internationales en charge de la lutte contre l'argent sale [100].

Les gestionnaires de risques dans les banques émettent des critiques sur le fonctionnement et l'apport des outils de filtrage. La fréquence des faux positifs (c'est-à-dire des alertes déclenchées par une homonymie) les préoccupe tout particulièrement. Ils n'ont pas hésité à s'en plaindre auprès de l'équipe de fonctionnaires onusiens qui suit les travaux du « comité 1267 » et à déplorer le manque d'éléments d'identification pour certaines entrées sur la liste de l'ONU [101]. Exprimant leur frustration lors de la mise en œuvre des sanctions (gel des fonds), ils soulignent que ces lacunes augmentent « *le risque que des personnes dont le nom figure sur la liste ne soient pas repérées et que les sanctions soient appliquées à des personnes qui n'étaient pas visées* [102] ». Par ailleurs, certaines listes comprennent des informations erronées. Selon un rapport du ministère de la Justice américain, 24 000 personnes figureraient à tort sur la liste antiterroriste consolidée du FBI comprenant environ 400 000 individus, ce qui correspond à plus d'un million de noms et d'*alias* [103]. Certains gouvernements ont également conscience de problèmes inhérents aux listes commerciales utilisées par les banques afin de filtrer leurs relations clients : « *Pour une banque, l'investigation et l'évaluation sont quelque chose de coûteux, donc très souvent si un nom apparaît sur une liste commerciale telle que* WorldCheck, *elle va refuser la transaction de ce client sans effectuer de recherches additionnelles. Le problème est que les fournisseurs d'outils n'ont pas d'obligations de vigilance vis-à-vis des informations qu'ils tirent de sources publiques plus ou moins fiables et ils ne vérifient pas leurs données régulièrement. Par exemple, quelqu'un qui a été radié d'une liste officielle peut rester sur la liste* WorldCheck. *Donc il y a là un risque potentiel lié à la qualité des informations de ces vendeurs d'outils* [104] ». Les professionnels s'interrogent aussi sur leurs devoirs de vigilance vis-à-vis de personnes politiquement exposées dont la définition est imprécise : « *Regardez le délire des PPE ! Ca va chercher loin ! Le conjoint, c'est qui ? Comment sort-on de ces listes ?* [105] ». De même le respect des embargos pose de difficiles dilemmes pratiques en matière de surveil-

99 . D'après nos entretiens avec des responsables de l'anti-blanchiment dans des banques françaises.

100.Voir les résolutions 1737-2006 et 1747-2007 du Conseil de sécurité de l'ONU.

101.Conseil de sécurité des Nations unies 2008. L'équipe de suivi précise qu'au moment de la publication de ce rapport : « *57 entrées concernant des individus ne comportent pas de nom et de date de naissance complets ; 5 autres entrées comportent un nom complet et une date de naissance, sans plus ; et 26 entrées comportent un nom, une date et un lieu de naissance, mais aucun autre élément d'identification, comme une nationalité, une adresse ou un pays de résidence* ».

102.*Ibid.*

103.U.S. Department of Justice, Office of the Inspector General Audit Division, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, mai 2009.

104.Entretien avec un officiel britannique, Londres, janvier 2009.

105.Entretien avec un *chief compliance officer* dans un établissement bancaire, Paris, juin 2007.

lance : « *Le texte de la liste des produits sous embargo fait quinze pages ! S'il ne s'agissait que du matériel militaire et de défense, ça serait facile, mais, sur la liste* […] *on trouve des choses comme les boulons ou les centrifugeuses dentaires parce qu'ils pourraient être utilisés dans la construction de centrales !* [106] ». Comme nous le verrons, ces préoccupations ne trouvent cependant guère de relais hors du monde bancaire.

Les outils de la lutte contre l'argent sale proposent également des fonctions de profilage. Il s'agit de techniques d'analyse comportementale dont l'objectif est de détecter le fonctionnement inhabituel d'un compte, en construisant des types de personnes ou de situations à partir de données éparses. La corrélation de ces données et la constitution de groupes de pairs permettent de prédire le comportement d'un client et de distinguer ses écarts vis-à-vis de son profil. Les outils de profilage reflètent la transformation d'outils de séduction (destinés à attirer et conserver des clients) en outils de suspicion [107]. Ces outils ont d'abord été utilisés dans les banques pour analyser le comportement des usagers et repérer leurs besoins potentiels, avant de devenir des outils de sécurité financière [108]. Le rôle du profilage dans la gestion des risques au sein des banques a également évolué : initialement mobilisé en tant qu'outil d'aide à la décision concernant l'autorisation préalable des transactions, il fonde aujourd'hui l'« *appréhension globale du dossier d'un client* [109] ».

Les opérations de profilage s'appuient sur des paramètres qui correspondent à des injonctions réglementaires précises (par exemple, la définition d'un seuil de transaction à partir duquel la vigilance bancaire doit être renforcée) ou qui sont définis selon les priorités de l'établissement, par l'intermédiaire des responsables de la conformité. Ces derniers disposent donc d'une latitude importante pour définir les profils suspects et les paramètres de manière intuitive, en lien avec l'actualité médiatique : « *Il y a les initiatives centrales* [*i.e.* au niveau de la direction de l'établissement bancaire] *: on prend un secteur, par exemple le recyclage de métaux, et on regarde tous les dossiers où apparaît cette activité. Il y a aussi mes initiatives : moi, maintenant, j'ai envie de regarder les sociétés de sécurité : j'ai lu un article sur les liens entre entreprises de sécurité et salafisme. Je suis un dévoreur de presse. Il y a aussi tout ce qui tourne autour de la fraude à la TVA : je regarderais bien les galeries d'art…* [110] ». Les *chief compliance officers* distinguent non seulement les secteurs d'activité à risque, mais aussi les zones géographiques qui, selon eux, sont particulièrement expo-

106.Entretien avec un *chief compliance officer* dans un établissement bancaire, Paris, octobre 2008.
107.Sur les notions de *categorical seduction* et de *categorical suspicion*, cf. Lyon D., *Surveillance Studies : An Overview*, Cambridge, Polity Press, 2007, pp. 102-108.
108.Canhoto A. I., "Profiles in Context: Analysis of the Development of a Customer Loyalty Program and of a Risk Scoring Practice" in Hildebrandt M., Gutwirth S. (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht, Springer, 2008, pp. 211-215.
109.Canhoto A. I., *Profiling Behaviour : the Social Construction of Categories in the Detection of Financial Crime*, Londres, London School of Economics, rapport 2007, p. 25.
110.Entretien avec un *chief compliance officer*, Paris, juin 2007.

sées aux pratiques de blanchiment. Les techniques de profilage accordent ainsi une place importante aux pays à risque qui apparaissent dans les transactions et rejoignent, sur ce point, les préoccupations à l'œuvre dans les opérations de filtrage. Les stéréotypes sur les pays étrangers, par exemple dans le continent africain ou dans la zone post-communiste, sont nombreux chez les *chief compliance officers* que nous avons interrogés.

En France comme dans les pays anglo-saxons, les pratiques de profilage ne suscitent guère de controverses. En dehors de travaux universitaires qui pointent les risques de discrimination au sein de la clientèle [111] et s'intéressent, de façon plus générale, aux problématiques de la protection de la vie privée mise en cause par les possibilités contemporaines de *dataveillance* [112], la critique reste cantonnée aux professionnels de la finance en charge de ces dossiers. Ils émettent fréquemment des doutes sur la pertinence de ces outils, notamment sur la validité des données utilisées et des corrélations établies afin de définir les profils : « *Sans même parler d'algorithmes complexes, prenez les attentats de 2005 à Londres, certains membres du commando ont été identifiés et une société de conseil a soumis l'idée de paramétrer notre système de détection sur leur profil client. Mais ce profil était virtuellement le même que n'importe quel étudiant du pays, c'est extrêmement dangereux de tirer des conclusions sur des typologies aussi larges !* [113] ». Alors qu'elles marquent l'intégration du monde bancaire dans des missions gouvernementales de surveillance, les opérations de profilage se caractérisent par leur invisibilité et leur incapacité à être érigées en enjeu du débat public. Elles constituent l'une des boîtes noires des dispositifs élaborés au nom de la lutte contre le blanchiment et le financement du terrorisme.

Dans le cas français, la critique de la diffusion et de l'usage des outils de surveillance (filtrage et profilage) reste principalement limitée aux professionnels, mais la CNIL a néanmoins engagé une réflexion sur cette question dès 2003. Comme le souligne un membre de cette institution, « [Quand on voit] *toutes ces listes commerciales qui se sont développées... La CNIL est l'une des rares autorités à s'être intéressée à ces données. Ce problème sinon n'intéresse que les banquiers !* [114] ». De par le caractère pionner de sa vigilance vis-à-vis de cet enjeu, mais aussi de par sa faible capacité à tenir sa position face aux impératifs de la lutte contre le terrorisme, l'activité de la CNIL livre des enseignements généraux sur la critique des outils de surveillance.

111.Schauer F., *Profiles, Probabilities and Stereotypes*, Cambridge, Harvard University Press, 2003.

112.Levi M., Wall D., "Technologies, Security and Privacy in post-9/11 European Information Society", *op.cit.*.

113.Entretien avec un *chief compliance officer* dans un établissement bancaire, Londres, décembre 2008.

114.Entretien à la CNIL, juin 2009.

Critique des dispositifs bancaires : le cas de la CNIL

Dès 2003, la Commission rédige un rapport sur les enjeux des dispositifs bancaires de lutte contre l'argent sale pour la « vie privée » des clients [115]. Constatant que les organismes financiers sont soumis à un devoir d'alerte qui les conduit à exercer un « *contrôle accru sur les activités de leurs clients* », la CNIL s'intéresse notamment à « *l'utilisation de traitements automatisés relatifs à la surveillance* » des personnes et des comptes bancaires, c'est-à-dire à la fois aux instruments de filtrage et de profilage. Le développement d'un marché des outils de détection des PPE l'inquiète spécifiquement [116].

La CNIL rappelle aux établissements financiers leurs devoirs eu égard à la législation sur la protection des données personnelles. Elle perçoit plusieurs risques liés à l'usage des outils. D'abord celui d'un usage « disproportionné » de ces instruments qui conduirait automatiquement les établissements à prendre des décisions potentiellement graves pour les clients. Celui, ensuite, de conduire à ne pas respecter la confidentialité des informations, alors que nul établissement n'est « *habilité à transmettre à des tiers des données nominatives concernant sa clientèle* [117] ». Enfin, celui d'un « *détournement de finalité* […] *à des fins de prospection commerciale* [118] ». Ce dernier point reflète une hypothèse fréquemment avancée par les responsables publics de la lutte anti-blanchiment afin d'expliquer l'investissement des banques dans la lutte contre l'argent sale. Cette hypothèse consiste à penser que les banques compenseraient le coût considérable de l'équipement contre le blanchiment et le financement du terrorisme par les profits tirés d'une meilleure connaissance de la clientèle, permettant ainsi de cibler au plus près leurs attentes et besoins. Le traitement des données sur les clients reviendrait ainsi paradoxalement à sa vocation première, une finalité commerciale, après avoir temporairement servi à des objectifs de surveillance. Le cas français ne semble cependant pas confirmer cette hypothèse : à une ou deux exceptions près revendiquant ce type de pratiques, les responsables de l'anti-blanchiment dans les banques considèrent l'équipement contre l'argent sale uniquement comme un coût.

Malgré un engagement précoce, la CNIL a dû composer avec les exigences prioritaires de la lutte contre le blanchiment et le financement du terrorisme. L'appel à limiter la circulation internationale de données personnelles semble par exemple dépassé. L'enjeu peine d'ailleurs à s'imposer au sein même de cette institution, car nombre de commissaires considèrent que l'investisse-

115.CNIL, *La lutte contre le blanchiment d'argent et le financement du terrorisme au sein des organismes financiers : quels enjeux pour la vie privée de la clientèle bancaire ?* Rapport d'étape adopté en séance plénière le 7 octobre 2003.

116.La CNIL se soucie particulièrement de la présence de données sur les condamnations ou sur les procédures judiciaires concernant les PPE. Entretien CNIL, juin 2009.

117.CNIL, *La lutte contre le blanchiment d'argent et le financement du terrorisme au sein des organismes financiers…*, *op.cit.*, p. 17.

118.*Ibid.*, p. 15.

ment dans ce domaine est voué à être improductif [119]. Il en est de même au niveau européen où le sujet n'apparaît pas non plus dans les travaux du G 29. La CNIL limite son activité à garantir des procédures transparentes de droit d'accès indirect à des informations relatives aux comptes bancaires détenues par les établissements. Cette procédure permet à un plaignant de demander à la CNIL d'avoir accès à de telles informations [120], ce qui préalablement ne concernait que les fichiers de police. Dans la pratique, le dépôt de plaintes ne se limite toutefois qu'à quelques cas, car le public connaît encore mal cette procédure [121]. En outre, depuis 2008, la CNIL reçoit de plus en plus fréquemment des plaintes de particuliers qui dénoncent les demandes d'information adressées par leur banque : « *Les plaintes sont formulées dans le genre : "on me demande des éléments d'information hors sujet, hors propos" ; "Mon banquier m'a opposé un argument d'autorité" ; "J'ai reçu un questionnaire qui passait en force. J'ai cru avoir affaire au fisc"… La relation au banquier est aujourd'hui en train de changer. On passe d'une relation de partenariat, d'accompagnement, de conseil à des exigences tatillonnes. Certains plaignants estiment que les banques se comportent "comme une administration"…* [122] ». L'AFUB (Association française des usagers de banques) a d'ailleurs saisi la CNIL dans ce sens en dénonçant le contenu des questionnaires-clients envoyés par les banques au titre du décret de septembre 2009 relatif à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Appelant à boycotter ces formulaires jugés abusifs et à « *dire non à cette inquisition* », la porte-parole de l'association précise que l'AFUB ne « *voit pas le rapport entre le nombre d'enfants des clients – une question posée dans les lettres des banques – et la lutte contre le terrorisme ou le blanchiment d'argent* [123] ». En aucun cas les plaintes ne portent sur des faits de discrimination. De son côté, la HALDE (Haute autorité de lutte contre les discriminations et pour l'égalité) n'a pas connaissance de cas d'abus liés à l'usage des outils de la lutte contre l'argent sale dans les banques. La critique des effets de l'anti-blanchiment dans les banques peine donc à s'appuyer sur des cas visibles, illustrant concrètement les dangers des dispositifs mis en place pour le client lambda.

***

119. Entretien CNIL, juin 2009.

120. Arrêté du ministère du budget, des comptes publics et de la fonction publique du 13 décembre 2007 modifiant l'arrêté du 14 juin 1982 fixant les modalités d'extension d'un système automatisé de gestion du fichier des comptes bancaires (http://admi.net/jo/20080112/BCFL0774627A.html). Cet arrêt fait suite à un avis de la CNIL du 4 octobre 2007.

121. Certains observateurs considèrent que le nombre de demandes pourrait pourtant augmenter du fait de l'extension de la lutte anti-blanchiment dans les banques aux infractions fiscales résultant de la transposition par la France de la troisième directive européenne sur ce sujet. Ordonnance n° 2009-104 du 30 janvier 2009 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et de financement du terrorisme.

122. Entretien CNIL, juin 2009.

123. *Agence France-Presse* (AFP), « Appel à boycotter des questionnaires de banques trop indiscrets », 4 février 2010.

Plusieurs facteurs peuvent permettre d'expliquer la variation des mobilisations selon les pratiques de surveillance décrites. La formulation du problème que posent les « listes noires » est relativement simple. Le combat s'inscrit dans la défense d'une cause qui consiste à contester la légitimité des mesures gouvernementales adoptées au nom de la lutte contre le terrorisme. La dénonciation de l'ingérence de l'Etat dans la vie quotidienne se superpose souvent à une vision du monde critiquant la domination qu'a pu exercer l'administration Bush sur la définition de normes de conduite globales. En outre, les effets de ces listes ont la particularité d'être tangibles et parlants pour tous les citoyens, puisqu'ils touchent à des libertés individuelles auxquelles chacun peut s'identifier : droit de préserver sa dignité, de circuler, d'avoir des revenus, d'exercer une activité économique, etc. Les mobilisations contre les conséquences des listes noires consistent ainsi à prendre la défense des individus contre les excès de surveillance d'un gouvernement global.

Bien que l'affaire SWIFT partage des traits communs, l'enjeu est moins évident à formuler. Il est en effet beaucoup plus difficile de s'identifier aux victimes parce que les modes d'utilisation des informations transmises ne sont pas connus et que les effets de leur dévoilement ne sont pas tangibles. Et ce n'est pas l'invocation des risques d'espionnage économique qui peut parvenir à susciter l'indignation des défenseurs des droits de l'Homme. La mobilisation peine donc à se développer, voire même suscite l'hostilité dans des conditions où les victimes sont floues, les dommages qui leur sont causés incertains et les responsabilités « *profondément entremêlées et difficiles à discerner* [124] ». Bien que la sphère des médias ait incontestablement joué le rôle de lanceur d'alerte dans ce cas précis, son pouvoir de mise en visibilité n'a pas permis d'étendre une affaire qui reste limitée à deux camps antagonistes aux périmètres institutionnel et sectoriel bien circonscrits. Les révélations médiatiques ne sauraient donc suffire à assurer une réaction collective et en cela ne constituent pas un facteur décisif pour comprendre l'issue d'une affaire quelle qu'elle soit.

Enfin, l'usage d'instruments de surveillance dans les banques est loin de susciter le même intérêt que les « listes noires », comme s'il révélait une incapacité à en formuler clairement les enjeux pour les citoyens. Le développement de la surveillance bancaire a beau mettre à l'épreuve les frontières de l'Etat, notamment l'organisation des missions de police et de renseignement, il ne suscite qu'un faible engouement du public et des médias. Ce décalage est d'autant plus paradoxal que les listes noires internationales concernent un nombre restreint de personnes (environ 500 dans la liste de l'ONU) alors que les pratiques de surveillance mises en place dans les banques touchent potentiellement tout un chacun [125]. Le silence qui entoure l'usage des instruments dans les banques peut s'expliquer de diverses manières. La plus triviale

124.Lascoumes P., *Elites irrégulières. Essai sur la délinquance d'affaires*, Paris, Flammarion, 1997.
125.Mentionnée précédemment dans cet article, la liste FBI n'a de valeur qu'aux Etats-Unis.

consiste à l'imputer à l'invisibilité qui caractérise les pratiques de surveillance bancaire [126]. Les informations que traitent ces instruments ne sont en effet *a priori* connues qu'en interne dans les établissements, ainsi que par les acteurs policiers et judiciaires concernés. Cependant, d'autres pratiques de surveillance tout aussi invisibles éveillent davantage l'intérêt d'une « opinion critique », comme l'illustre par exemple l'hostilité au système Echelon.

Une autre hypothèse consiste à considérer que la difficile problématisation de cet enjeu est liée au fait que ce n'est pas l'Etat mais les établissements financiers privés qui surveillent les transactions. Or, les mobilisations pour la protection des données personnelles visent en général à dénoncer l'ingérence du gouvernement dans la vie privée des citoyens. L'Etat ne détient certes pas le monopole de la surveillance : les grandes entreprises peuvent chercher à mieux connaître leurs employés afin de les encadrer, et leurs clients afin d'adapter leur offre à la demande de consommation [127]. Mais le fait que le gouvernement et des établissements privés puissent s'engager ensemble dans des « *assemblages de surveillance* [128] » au nom d'objectifs communs échappe à une grille d'analyse où les finalités étatiques et commerciales de la collecte d'informations personnelles semblent inconciliables. Les banques sont vues comme des entités commerciales et non comme des bras armés de l'Etat dans la lutte contre l'argent sale. Le rôle que jouent depuis deux décennies les établissements financiers privés dans la conduite des politiques pénales (lutte contre la drogue, la corruption, le terrorisme, etc.) semble encore largement ignoré du grand public.

Une dernière hypothèse peut être formulée dans la continuité de la précédente. La faible mobilisation contre l'usage des outils de filtrage et de profilage dans les banques peut s'expliquer par le fait que les acteurs militant contre l'ingérence de l'Etat dans la vie privée des citoyens critiquent aussi fréquemment les dérives du capitalisme financier, tel qu'il s'est développé dans les dernières décennies. Dans les années 2000, les milieux altermondialistes, voués à combattre les méfaits de la « mondialisation financière », se sont fréquemment investis dans la dénonciation des dispositifs de surveillance mis en place par l'administration Bush pour lutter contre le terrorisme. Il est donc difficile d'imaginer qu'ils plaident en faveur d'un renforcement du secret bancaire pour défendre les libertés individuelles.

126.Cf. par exemple le discours prononcé par Alex Türk, président de la CNIL, lors de la conférence internationale des commissaires à la protection des données qui s'est tenue à Londres en novembre 2006. Discours reproduit dans CNIL, *27e rapport d'activité*, Paris, La Documentation française, 2006 : « *Le premier facteur d'invisibilité résulte de la multiplication des traitements qui, s'ils sont effectués par des technologies visibles physiquement, sont toutefois réalisés à l'insu des personnes, si bien qu'ils sont, en pratique, pour celles-ci, parfaitement invisibles* ».

127.Sur ces points, cf. Lyon D., *Surveillance Studies: An Overview*, *op.cit.*, pp. 33-36 et 40-44.

128.Haggerty K. D., Ericson R. V., "The Surveillant Assemblage", *British Journal of Sociology*, vol. 51, n° 4, décembre 2000, pp. 605-622.

Si la critique de la surveillance bancaire ne débouche pas sur une mobilisation significative, c'est qu'elle est avant tout prise en charge par les professionnels concernés. Les milieux financiers dénoncent à l'envi les excès de la surveillance dans un but corporatiste de défense de l'activité financière. Dans un éditorial intitulé « Le secret bancaire joue aussi un rôle éthique », un responsable du groupe de Riencourt, un think tank libéral suisse, s'étonne d'ailleurs que « la gauche » ne se préoccupe pas de cet enjeu : « *Au regard de la protection de la sphère privée et de la menace de fichage brandie par certains, il apparaît beaucoup plus urgent de défendre le secret bancaire que de s'attaquer aux nouveaux documents d'identité. De même, les défenseurs de la protection de la sphère privée sur Internet ne peuvent pas simplement passer sous silence celle du secret bancaire* [129] ». Loin de vouloir clore la controverse, ces acteurs cherchent au contraire à l'élargir mais en s'attachant à la formuler dans un espace de calcul qui leur est propre et bénéfique. Avec l'extension du champ des professions impliquées dans la lutte contre l'argent sale en Europe, suite à l'adoption de la troisième directive anti-blanchiment de l'UE, cette critique est aujourd'hui également reprise par les notaires et les avocats, au nom du respect des droits fondamentaux.

De leur côté, les ONG et les institutions mobilisées pour sauvegarder les libertés individuelles sont en difficulté face à la problématisation d'un enjeu qui passe par la défense des établissements financiers privés. La grille d'analyse qu'ils apposent à cet enjeu les conduit à le réduire à une tension préoccupante entre le renforcement des mesures gouvernementales pour lutter contre des menaces jugées exceptionnelles et la protection des libertés individuelles. Comme l'illustre le rapport de la CNIL publié en 2003 : « *Comment inscrire dans un juste équilibre d'une part, la recherche de sécurité et l'ensemble des vigilances indispensables à la lutte contre la délinquance financière, d'autre part, le respect du droit des personnes et la protection de la vie privée ? Telle est la difficile équation à résoudre* [130] ». Une telle formulation ne laisse guère de place aux intermédiaires privés qui mettent en œuvre la politique gouvernementale. Doit-on défendre le secret bancaire pour protéger les citoyens contre les excès de la surveillance gouvernementale ? L'existence de deux positions critiques difficilement conciliables, associées à des univers professionnels distincts, pèse sur le développement d'une mobilisation contre la surveillance opérée par les institutions financières privées au nom d'objectifs gouvernementaux.

129.*Le Temps*, « Le secret bancaire joue aussi un rôle éthique », 10 août 2009.
130.CNIL, *La lutte contre le blanchiment d'argent et le financement du terrorisme au sein des organismes financiers…*, *op.cit.*, p. 11.